IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PACSEC3, LLC,	)	
Plaintiff,	)	
	)	**Civil Action No. 6:21-cv-00388**
v.	)	
	)	
CISCO SYSTEMS, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

PacSec3, LLC ("PacSec") files this Original Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent Nos. 6,789,190 ("the '190 patent"); 7,047,564 ("the '564 patent"); and, 7,523,497 ("the '497 patent") (collectively referred to as the "Patents-in-Suit") by Cisco Systems, Inc.

I. THE PARTIES

1. Plaintiff PacSec3, LLC is a Texas Limited Liability Company with its principal place of business located in Harris County, Texas.

2. On information and belief, Cisco Systems, Inc. ("Cisco") is a California Corporation. On information and belief, CISCO sells and offers to sell products and services throughout Texas, including in this judicial district, and introduces products and services that perform infringing methods or processes into the stream of commerce knowing that they would be sold in Texas and this judicial district. CISCO can be served with process through their Registered Agent, Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218 or wherever they may be found.

II. JURISDICTION AND VENUE

3. This Court has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because Plaintiff's claim arises under an Act of Congress relating to patents, namely, 35 U.S.C. § 271.

4. This Court also has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. § 1332(a)(1) because Plaintiff is a limited liability company organized under the laws of the State of Texas and Defendant is a California Corporation with a principal, physical place of business at 300 East Tasman Dr. San Jose, CA 95134. The matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs.

5. This Court has personal jurisdiction over Defendant because: (i) Defendant is present within or has minimum contacts within the State of Texas and this judicial district; (ii) Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in this judicial district; and (iii) Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas and in this judicial district.

6. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b). Defendant has committed acts of infringement and has a regular and established place of business in this District. Further, venue is proper because Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in Texas and this District.

III. INFRINGEMENT

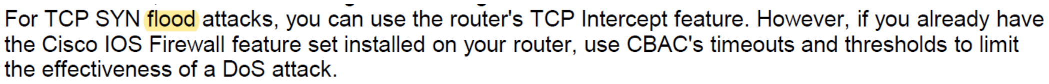
A. Infringement of the '190 Patent

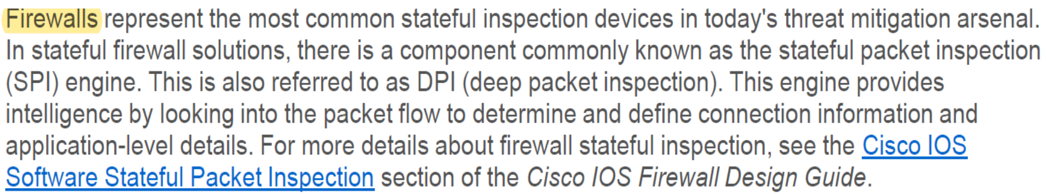
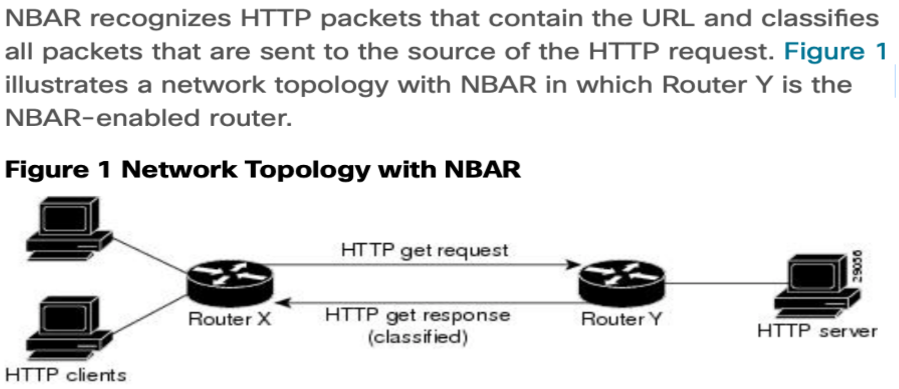
7. On September 7, 2004, U.S. Patent No. 6,789,190 ("the '190 patent," attached as Exhibit A) entitled "PACKET FLOODING DEFENSE SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '190 patent by assignment.

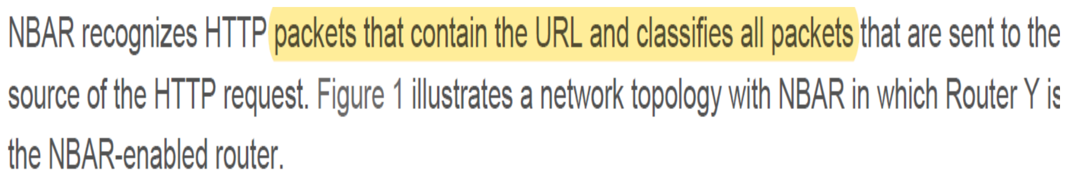
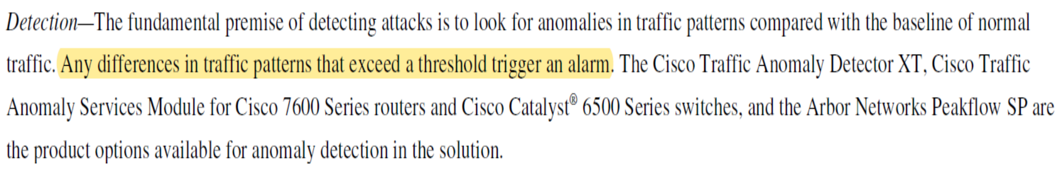
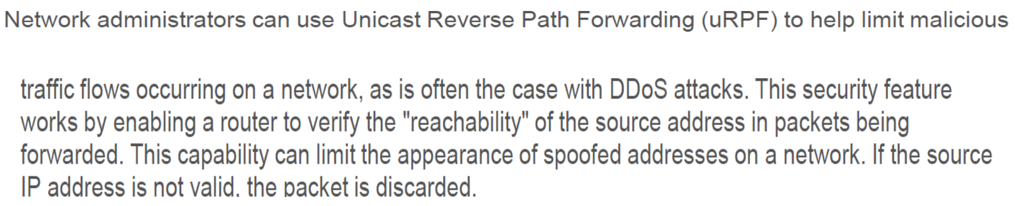
8. The '190 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

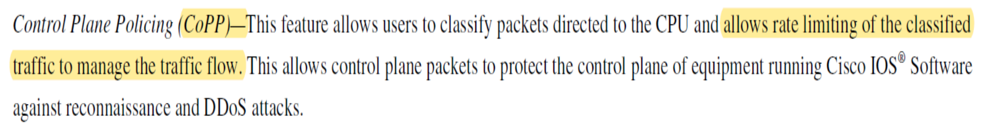
9. CISCO offers for sale, sells and manufactures one or more firewall systems that infringes one or more claims of the '190 patent, including one or more of claims 1-3, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the '190 Patent into service (i.e., used them); but for Defendant's actions, the claimed-inventions embodiments involving Defendant's products and services would never have been put into service. Defendant's acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant's procurement of monetary and commercial benefit from it.

10. Support for the allegations of infringement may be found in the following preliminary table:

Exemplary Claim language	**Cisco Evidence**
A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system	 For TCP SYN flood attacks, you can use the router's TCP Intercept feature. However, if you already have the Cisco IOS Firewall feature set installed on your router, use CBAC's timeouts and thresholds to limit the effectiveness of a DoS attack. **Cisco Router Firewall Security: DoS Protection | Detecting DoS Attacks (Page 24)** Cisco DDoS Protection has a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.

comprising: at least one firewall, said firewall comprising:	 Firewalls represent the most common stateful inspection devices in today's threat mitigation arsenal. In stateful firewall solutions, there is a component commonly known as the stateful packet inspection (SPI) engine. This is also referred to as DPI (deep packet inspection). This engine provides intelligence by looking into the packet flow to determine and define connection information and application-level details. For more details about firewall stateful inspection, see the Cisco IOS Software Stateful Packet Inspection section of the *Cisco IOS Firewall Design Guide*. **A Cisco Guide to Defending Against Distributed Denial of Service Attacks (Page 16)**
… hardware and software serving to control packet transmission between said network and a host computer connected to an internal network;	 NBAR recognizes HTTP packets that contain the URL and classifies all packets that are sent to the source of the HTTP request. Figure 1 illustrates a network topology with NBAR in which Router Y is the NBAR-enabled router. **Figure 1 Network Topology with NBAR** HTTP get request HTTP get response (classified) Router X Router Y HTTP server HTTP clients 29036 **Classifying Network Traffic Using NBAR (Page 6)** The reference describes at least one firewall [Firewalls], said firewall comprising: hardware and software serving to control packet transmission between said network and a host computer connected to an internal network [Router X + Router Y].

… means for classifying data packets received at said firewall;,…	 NBAR recognizes HTTP packets that contain the URL and classifies all packets that are sent to the source of the HTTP request. Figure 1 illustrates a network topology with NBAR in which Router Y is the NBAR-enabled router. **Classifying Network Traffic Using NBAR (Page 6)**
means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall  *Detection*—The fundamental premise of detecting attacks is to look for anomalies in traffic patterns compared with the baseline of normal traffic. Any differences in traffic patterns that exceed a threshold trigger an alarm. The Cisco Traffic Anomaly Detector XT, Cisco Traffic Anomaly Services Module for Cisco 7600 Series routers and Cisco Catalyst® 6500 Series switches, and the Arbor Networks Peakflow SP are the product options available for anomaly detection in the solution. **CISCO DDOS PROTECTION SOLUTION—DELIVERING "CLEAN PIPES" CAPABILITIES FOR SERVICE PROVIDERS AND THEIR CUSTOMERS (Page 4)**
means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall; and	 Network administrators can use Unicast Reverse Path Forwarding (uRPF) to help limit malicious traffic flows occurring on a network, as is often the case with DDoS attacks. This security feature works by enabling a router to verify the "reachability" of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. **A Cisco Guide to Defending Against Distributed Denial of Service Attacks (Page 17)**

	The reference describes means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall [enabling a router to verify the "reachability" of the source address in packets being forwarded].
whereby, said firewall can use said information to allocate the transmission rate for each class in a desired way.	 *Control Plane Policing (CoPP)*—This feature allows users to classify packets directed to the CPU and allows rate limiting of the classified traffic to manage the traffic flow. This allows control plane packets to protect the control plane of equipment running Cisco IOS® Software against reconnaissance and DDoS attacks. **CISCO DDOS PROTECTION SOLUTION—DELIVERING "CLEAN PIPES" CAPABILITIES FOR SERVICE PROVIDERS AND THEIR CUSTOMERS (Page 6)**

These allegations of infringement are preliminary and are therefore subject to change.

11. CISCO has and continues to induce infringement. CISCO has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–3 of the '190 patent, literally or under the doctrine of equivalents. Moreover, CISCO has known of the '190 patent and the technology underlying it from at least the date of issuance of the patent.

12. CISCO has and continues to contributorily infringe. CISCO has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–3 of the '190 patent, literally or under the doctrine of

equivalents. Moreover, CISCO has known of the ‘190 patent and the technology underlying it from at least the date of issuance of the patent.

13. CISCO has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the ’190 patent.

B. Infringement of the ’564 Patent

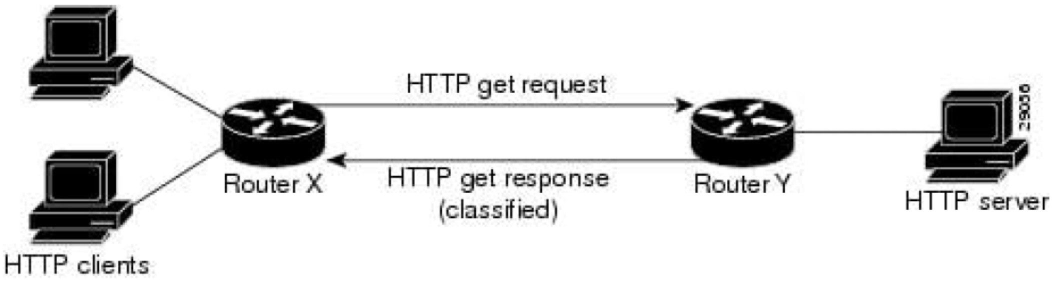
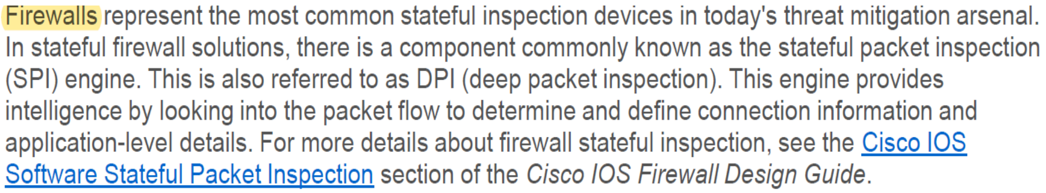
14. On May 16, 2006, U.S. Patent No. 7,047,564 (“the ‘564 patent”, attached as Exhibit B) entitled “REVERSIBLE FIREWALL PACKET TRANSMISSION CONTROL SYSTEM,” was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the ‘564 patent by assignment.

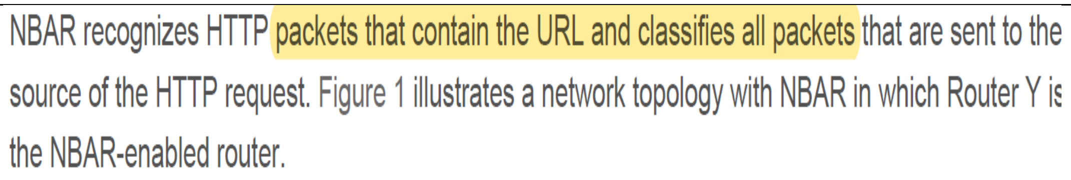
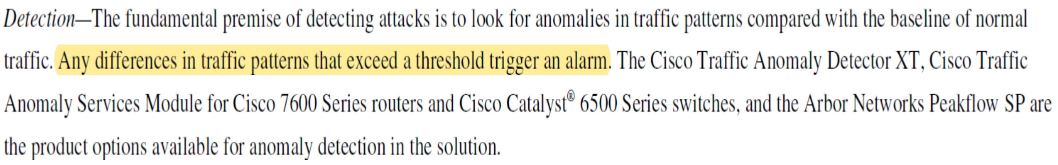
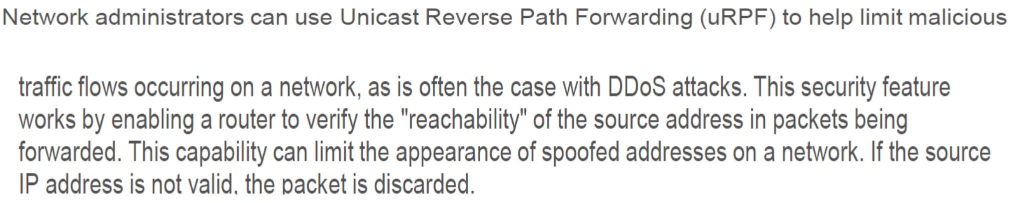
15. The ‘564 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

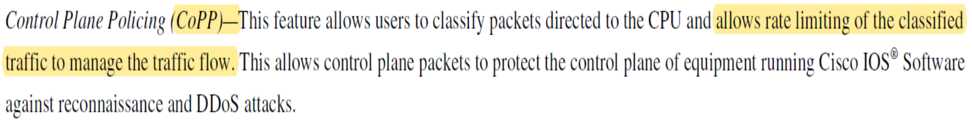
16. CISCO offers for sale, sells and manufactures one or more firewall systems that infringes one or more claims of the ‘564 patent, including one or more of claims 1-6, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the ‘564 Patent into service (i.e., used them); but for Defendant’s actions, the claimed-inventions embodiments involving Defendant’s products and services would never have been put into service. Defendant’s acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant’s procurement of monetary and commercial benefit from it.

17. Support for the allegations of infringement may be found in the following preliminary table:

Exemplary Claim language	**Cisco Evidence**

A packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host computers, communication lines and transmitted data packets, said system comprising:	The reference describes packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host computers, communication lines and transmitted data packets, **Figure 1 Network Topology with NBAR**  HTTP get request Router X HTTP get response (classified) Router Y HTTP server HTTP clients 29036 **Classifying Network Traffic Using NBAR (Page 6)**
at least one firewall, said firewall comprising: hardware and software providing a non-redundant connection between said networks and serving to control packet transmission between said networks;	 Firewalls represent the most common stateful inspection devices in today's threat mitigation arsenal. In stateful firewall solutions, there is a component commonly known as the stateful packet inspection (SPI) engine. This is also referred to as DPI (deep packet inspection). This engine provides intelligence by looking into the packet flow to determine and define connection information and application-level details. For more details about firewall stateful inspection, see the Cisco IOS Software Stateful Packet Inspection section of the *Cisco IOS Firewall Design Guide*. **A Cisco Guide to Defending Against Distributed Denial of Service Attacks (Page 16)**
means for classifying data packets received at said firewall related to the	

consumption of at least one resource;	 NBAR recognizes HTTP packets that contain the URL and classifies all packets that are sent to the source of the HTTP request. Figure 1 illustrates a network topology with NBAR in which Router Y is the NBAR-enabled router. **Classifying Network Traffic Using NBAR (Page 6)** The reference describes means for classifying data packets received at said firewall related to the consumption of at least one resource [classifies all packets that are sent to the source of the HTTP request].
means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall  *Detection*—The fundamental premise of detecting attacks is to look for anomalies in traffic patterns compared with the baseline of normal traffic. Any differences in traffic patterns that exceed a threshold trigger an alarm. The Cisco Traffic Anomaly Detector XT, Cisco Traffic Anomaly Services Module for Cisco 7600 Series routers and Cisco Catalyst® 6500 Series switches, and the Arbor Networks Peakflow SP are the product options available for anomaly detection in the solution. **CISCO DDOS PROTECTION SOLUTION—DELIVERING "CLEAN PIPES" CAPABILITIES FOR SERVICE PROVIDERS AND THEIR CUSTOMERS (Page 4)**
means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet; and	 Network administrators can use Unicast Reverse Path Forwarding (uRPF) to help limit malicious traffic flows occurring on a network, as is often the case with DDoS attacks. This security feature works by enabling a router to verify the "reachability" of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. **A Cisco Guide to Defending Against Distributed Denial of Service Attacks (Page 17)** The reference describes means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet [Unicast Reverse Path Forwarding (uRPF) to help limit malicious traffic flows occurring on a network].

whereby, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection.	 *Control Plane Policing (CoPP)*—This feature allows users to classify packets directed to the CPU and allows rate limiting of the classified traffic to manage the traffic flow. This allows control plane packets to protect the control plane of equipment running Cisco IOS® Software against reconnaissance and DDoS attacks. **CISCO DDOS PROTECTION SOLUTION—DELIVERING "CLEAN PIPES" CAPABILITIES FOR SERVICE PROVIDERS AND THEIR CUSTOMERS (Page 6)** The reference describes packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection [classify packets directed to the CPU and allows rate limiting of the classified traffic to manage the traffic flow].

These allegations of infringement are preliminary and are therefore subject to change.

18. CISCO has and continues to induce infringement. CISCO has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–6 of the '564 patent, literally or under the doctrine of equivalents. Moreover, CISCO has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

19. CISCO has and continues to contributorily infringe. CISCO has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–6 of the '564 patent, literally or under the doctrine of equivalents. Moreover, CISCO has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

20. CISCO has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the ’564 patent.

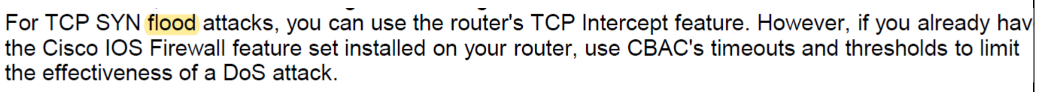
C. Infringement of the ‘497 Patent

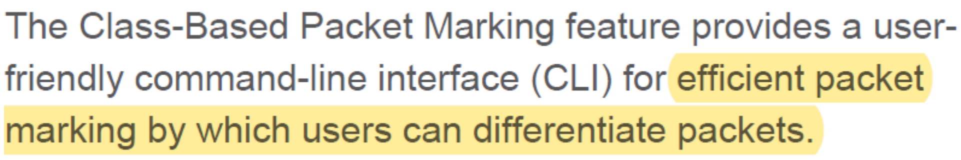
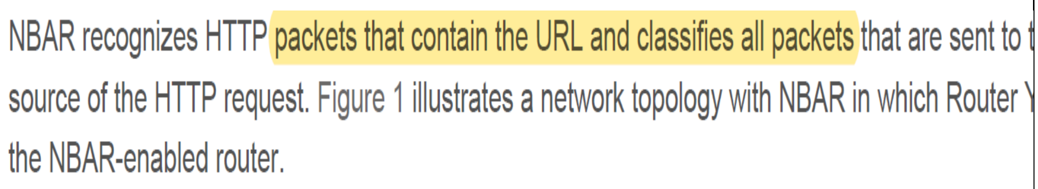
21. On April 21, 2009, U.S. Patent No. 7,523,497 (“the ‘497 patent”, attached as Exhibit C) entitled “PACKET FLOODING DEFENSE SYSTEM,” was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the ‘497 patent by assignment.

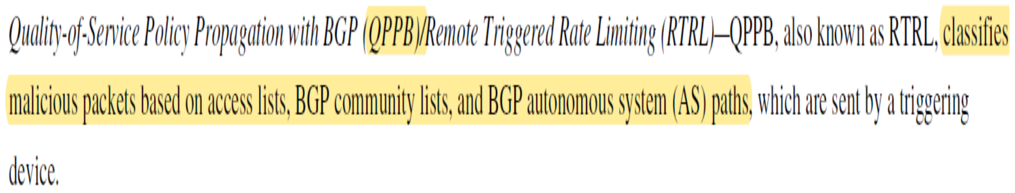
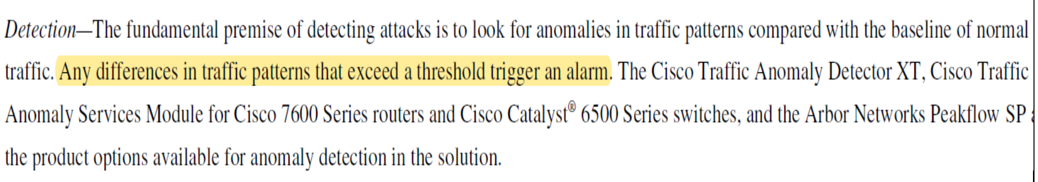
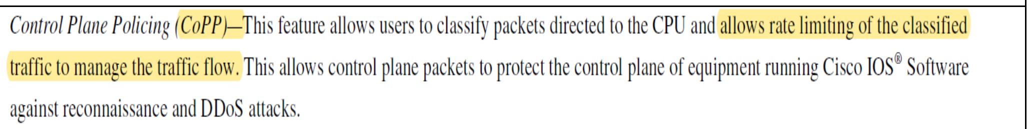
22. The ’497 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

23. CISCO offers for sale, sells and manufactures one or more firewall systems that infringes one or more claims of the ‘497 patent, including one or more of claims 1-18, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the ‘497 Patent into service (i.e., used them); but for Defendant’s actions, the claimed-inventions embodiments involving Defendant’s products and services would never have been put into service. Defendant’s acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant’s procurement of monetary and commercial benefit from it.

24. Support for the allegations of infringement may be found in the following preliminary table:

Exemplary Claim language	**Cisco Evidence**
A method of providing packet flooding defense for a network comprising a plurality of	 For TCP SYN flood attacks, you can use the router's TCP Intercept feature. However, if you already hav the Cisco IOS Firewall feature set installed on your router, use CBAC's timeouts and thresholds to limit the effectiveness of a DoS attack.

host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:	**Cisco Router Firewall Security: DoS Protection | Detecting DoS Attacks (Page 24)** Cisco DDoS Protection has a method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.
determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;	 The Class-Based Packet Marking feature provides a user-friendly command-line interface (CLI) for efficient packet marking by which users can differentiate packets. **QoS: Classification Configuration Guide, Cisco IOS XE Everest (Page 17)** The reference describes determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer [packet marking by which users can differentiate packets based on the designated markings].  NBAR recognizes HTTP packets that contain the URL and classifies all packets that are sent to t source of the HTTP request. Figure 1 illustrates a network topology with NBAR in which Router Y the NBAR-enabled router. **Classifying Network Traffic Using NBAR (Page 6)** The reference describes said path comprising all routers in said network via which said packets are routed to said computer [Router Y is the NBAR-enabled router].

classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	 *Quality-of-Service Policy Propagation with BGP (QPPB)/Remote Triggered Rate Limiting (RTRL)*—QPPB, also known as RTRL, classifies malicious packets based on access lists, BGP community lists, and BGP autonomous system (AS) paths, which are sent by a triggering device. **CISCO DDOS PROTECTION SOLUTION—DELIVERING "CLEAN PIPES" CAPABILITIES FOR SERVICE PROVIDERS AND THEIR CUSTOMERS (Page 6)** The reference describes classifying data packets received at said host computer into wanted data packets and unwanted data packets by path [classifies malicious packets based on access lists, BGP community lists, and BGP autonomous system (AS) paths, which are sent by a triggering device].
associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	 *Detection*—The fundamental premise of detecting attacks is to look for anomalies in traffic patterns compared with the baseline of normal traffic. Any differences in traffic patterns that exceed a threshold trigger an alarm. The Cisco Traffic Anomaly Detector XT, Cisco Traffic Anomaly Services Module for Cisco 7600 Series routers and Cisco Catalyst® 6500 Series switches, and the Arbor Networks Peakflow SP the product options available for anomaly detection in the solution. **CISCO DDOS PROTECTION SOLUTION—DELIVERING "CLEAN PIPES" CAPABILITIES FOR SERVICE PROVIDERS AND THEIR CUSTOMERS (Page 4)** The reference describes associating a maximum acceptable processing rate with each class of data packet received at said host computer [traffic patterns compared with the baseline of normal traffic. Any differences in traffic patterns that exceed a threshold trigger an alarm].
allocating a processing rate less than or equal to	 *Control Plane Policing (CoPP)*—This feature allows users to classify packets directed to the CPU and allows rate limiting of the classified traffic to manage the traffic flow. This allows control plane packets to protect the control plane of equipment running Cisco IOS® Software against reconnaissance and DDoS attacks.

said maximum acceptable processing rate for unwanted data packets.	**CISCO DDOS PROTECTION SOLUTION—DELIVERING "CLEAN PIPES" CAPABILITIES FOR SERVICE PROVIDERS AND THEIR CUSTOMERS (Page 6)** The reference describes packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection [classify packets directed to the CPU and allows rate limiting of the classified traffic to manage the traffic flow].

These allegations of infringement are preliminary and are therefore subject to change.

25. CISCO has and continues to induce infringement. CISCO has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the '497 patent, literally or under the doctrine of equivalents. Moreover, CISCO has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

26. CISCO has and continues to contributorily infringe. CISCO has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the '497 patent, literally or under the doctrine of equivalents. Moreover, CISCO has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

27. CISCO has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the '497 patent.

IV. JURY DEMAND

PacSec3 hereby requests a trial by jury on issues so triable by right.

V. PRAYER FOR RELIEF

WHEREFORE, PacSec3 prays for relief as follows:

a. enter judgment that Defendant has infringed the claims of the '190 patent, the '564 patent and the '497 patent through selling, offering for sale, manufacturing, and inducing others to infringe by using and instructing to use at least the Cisco DDOS Protection Solution, and perhaps other firewall/DDOS protection systems;

b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patents-in-Suit in an amount no less than a reasonable royalty or lost profits, together with pre-judgment and post-judgment interest and costs under 35 U.S.C. § 284;

c. award PacSec3 an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;

d. declare this case to be "exceptional" under 35 U.S.C. § 285 and award PacSec3 its attorneys' fees, expenses, and costs incurred in this action;

e. declare Defendant's infringement to be willful and treble the damages, including attorneys' fees, expenses, and costs incurred in this action and an increase in the damage award pursuant to 35 U.S.C. § 284;

f. a decree addressing future infringement that either (i) awards a permanent injunction enjoining Defendant and its agents, servants, employees, affiliates, divisions, and subsidiaries, and those in association with Defendant from infringing the claims of the Patents-in-Suit, or (ii) awards damages for future infringement in lieu of an injunction in an amount consistent with the fact that for future infringement the Defendant will be an adjudicated infringer of a valid patent, and trebles that amount in view of the fact that the future infringement will be willful as a matter of law; and

g. award PacSec3 such other and further relief as this Court deems just and proper.

Respectfully submitted,

Ramey & Schwaller, LLP

/s/William P. Ramey
William P. Ramey, III
Texas Bar No. 24027643
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
wramey@rameyfirm.com

Attorneys for PacSec3, LLC